



**DEPARTMENT OF THE ARMY**  
HEADQUARTERS, U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL  
AND FORT SAM HOUSTON  
2250 STANLEY ROAD  
FORT SAM HOUSTON, TEXAS 78234-6100

REPLY TO  
ATTENTION OF  
IMSW-SMH-IM

13 JUL 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Information Management Policy 25-02, Compromised  
Computer Systems

1. REFERENCE. Unclassified message, HQDA, SAIS-IOA, 172032Z Oct 01, subject: Compromised Computer Systems Policy and AR 25-2, Information Assurance, 14 Nov 2003.
2. PURPOSE. This policy clarifies actions required by users, as well as by system and network administrators in response to a system compromised by a worm, malicious code, or unauthorized access gained by an intruder.
3. SCOPE. This memorandum applies to all organizations located on Fort Sam Houston, Camp Bullis, and Camp Stanley that have connectivity to the installation network managed by the Director of Information Management (DOIM), and includes both Government-owned and leased automation equipment and any system authorized (such as contractor owned) or unauthorized (such as personal owned) equipment.
4. BACKGROUND. This policy was formulated to improve the security and reliability of the Fort Sam Houston computing environment and to ensure compliance with the references.
5. POLICY. If a system administrator or user suspects that a computer may have been compromised by a worm, malicious code, or unauthorized access has been gained by an intruder, he/she will take the following actions:
  - a. Do not turn the computer off.
  - b. The user will immediately isolate the system from the network and prevent all access to the system. Isolation includes physical isolation. Unplug the network connection and restrict any direct physical access to the wall jack.
  - c. The user will immediately contact the unit Information Assurance Security Officer (IASO), DOIM Help Desk (221-HELP) and stop anyone else from accessing the system.

IMSW-SMH-IM

SUBJECT: Installation Information Management Policy 25-02, Compromised Computer Systems

d. The user and unit IASO will immediately record their observations and the approximate time they noticed unusual activity, actions taken and the timeline of events and actions.

e. The DOIM Help Desk will immediately inform the Information Security section, Information Assurance Manager (IAM), and network administrators of a possible or ongoing network incident.

f. The systems administrator and the network administrator will immediately disable the switch port associated with the device.

g. The DOIM IAM or designated Information Security representative will immediately notify the supporting Regional Computer Emergency Response Team (RCERT), and make appropriate notifications to the Fort Sam Houston Information Assurance Officer and chain of command. Failure to notify the RCERT is a violation of Army regulations cited in the reference and could result in criminal or administrative disciplinary actions.

h. Army Computer Emergency Response Team (ACERT) or RCERT will provide guidance to the DOIM staff to obtain the forensic physical evidence required to support an investigation. The DOIM will be prepared to provide the system, but will not remove it until the lead investigative agency provides the guidance and requirements when directed by the investigator. The system will be attached to standalone isolation Virtual Local Area Network (VLAN) and a forensic copy of its hard drive will be made.

i. Once a system has been released for reuse to the DOIM, the hard drive will be reformatted using an approved low-level format method and the Operating System will be reinstalled and patched. The system's hard drive user(s) data will not be backed up, restored or returned to the user(s). This data is suspect and will not be allowed back on the network. The DOIM will conduct a vulnerability assessment and patch prior to bringing the system back online. The port block for the compromised system will be unblocked temporarily only to scan and will only be removed permanently after the system has had all identified vulnerabilities fixed and rescanned. Once certified for use, the system will be assigned from the standalone isolation VLAN to the production VLAN.

6. Systems verified as compromised with a known worm or through scripts that have automated scanning and installation processes are considered compromised systems and will be reported to RCERT. The DOIM will rebuild and patch compromised systems, even if an automated script that could install a backdoor, or Trojan Horse within the Operating System or applications, are not readily visible. All data are considered suspect

IMSW-SMH-IM


SUBJECT: Installation Information Management Policy 25-02, Compromised  
Computer Systems

and will not be archived and returned to the user. The use of any virus or malicious code removal tools will not be used to restore compromised systems. A clean install is the only acceptable security solution for any compromised systems. A vulnerability assessment will be conducted on the rebuilt system and only after it has been certified will the system return to the network.

7. Personal owned systems connected to the government network (see IM Policy 25-01) and infected with virus or malicious code will be confiscated and investigated for possible compromise. Criminal investigation may result from investigation. At a minimum, the system will be reformatted with a government approved tool prior to returning to user. Chain-of-command will discipline for misappropriating government resources.

8. This policy will be reviewed 2 years from the implementation date.

9. The point of contact is Mr. Jack D. Poland, Director of Information Management, 221-1300/5281, or email address [jack.poland1@us.army.mil](mailto:jack.poland1@us.army.mil).

  
RUSSELL J. OZERW  
Major General, DC  
Commanding

DISTRIBUTION:

A